IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al*.

Plaintiffs,

v.

BRAD RAFFENSPERGER, *et al.*,

Defendants.

FILED UNDER SEAL

CIVIL ACTION

FILE NO. 1:17-cv-2989-AT

STATE DEFENDANTS' RESPONSE TO COURT'S REQUEST ON DISCOVERY DISPUTE

GEMS DATABASE INSPECTION

The State Defendants have carefully evaluated the proposals during the Friday conference call with the Court regarding the request of both Plaintiff groups to inspect the GEMS Database. As this Court has recognized, and the parties discussed at length on Friday, the GEMS Database is a key component of Georgia's election system, which is "critical infrastructure" pursuant to 42 U.S.C. § 5195c.

Because of the extremely sensitive nature of this component of the election infrastructure in Georgia, the State takes significant efforts to secure the GEMS

Database and GEMS Server. At the deposition of Mr. Barnes on June 27, 2019, he detailed some (but not all) of those efforts:[1]

1. The GEMS Database is maintained on a server with extremely limited physical access, so that not even janitorial staff is allowed into the room where the server is located. (Deposition pp. 170:1-17).
2. The only access to the GEMS Server for the three ballot builders is through a hard-wired, private computer that is completely separate from the public computer used by the employee. (Deposition, pp. 29:4-17; 242:2-15).
3. The only external device that could access the GEMS Server is a single, lockable USB drive that is formatted before each use and is used to move PDF ballot proofs to a secure location for review by counties. (Deposition, pp. 176:11-178:10; 245:1-7).
4. Delivery of GEMS Databases to counties only happens through physical delivery of encrypted files on a CD—no electronic transfers are allowed. (Deposition, pp. 31:2-12; 33:2-4).

[1] The final deposition transcript is not yet completed for filing with the Court. Attached as Exhibit A are relevant portions of the rough draft transcript received from the court reporter.

5. The raw GEMS Database in Microsoft Access format is never transmitted to the counties. Instead, the only file sent to the counties is a GEMS file called a GBF file. (Deposition, pp. 192:13-193:16).
6. Counties do not proof the GEMS Database or view the Microsoft Access files except through the GEMS Application because Microsoft Access is not installed on the county GEMS Computers. (Deposition pp. 32:13-24; 193:6-16).

State Defendants have already offered multiple options for discovery that do not reveal the structure of the GEMS Database, including (1) extensive reports from the database, (2) GEMS Verify which tests to compare the executable files to a trusted version, and (3) a list of any macros within the database where any malicious code would appear. These options are far less dangerous ways of reviewing the data within the database without exposing the structure and other confidential information.

In response, Plaintiffs have not changed their basic position—they want the entire raw database file or nothing. This carte-blanche access to critical infrastructure, removed from all the protections surrounding the system, is akin to asking State Defendants to remove everything from a bank vault to test whether the things in the vault can be accessed. If Plaintiffs believe, as they said on the call on

Friday, that maintaining the raw GEMS Database files on an air-gapped system in a locked room is sufficient security, they are agreeing with the current security measures taken by the Secretary of State (whose security measures exceed what Plaintiffs propose) to secure this critical infrastructure.

As instructed by the Court on Friday, State Defendants have considered the options surrounding a possible inspection of the raw Access database. State Defendants propose the following structure for allowing a review in the Secretary of State's own environment without introducing anything foreign into that system.

PROPOSAL FOR REVIEW OF GEMS DATABASE

The Secretary of State's office will:

1. Create a server image with the same environment used in the counties, which will remain in a secure, air-gapped environment.
2. Load a copy of the GEMS Database from the November 2018 election.
3. Install Microsoft Access on the computer.
4. Remove the GEMS Application.
5. Allow Plaintiffs' expert to have supervised access in the Secretary of State's facility.

6. Plaintiffs will not be permitted to introduce any software or files onto the computer and will not be permitted to connect any hardware to the computer.
7. Plaintiffs will not be permitted to remove any files from the computer.
8. Plaintiffs will not be permitted to take pictures or videos of their review process.
9. Plaintiffs must make copies of all notes taken during the review and leave a copy of those notes with the Secretary of State's office except for attorney work product.

PROTECTIVE ORDER

The remaining issues with the protective order involve the application of the "attorneys' eyes only" ("AEO") provision to non-attorneys and whether a party can mark documents confidential after production by a non-party. Plaintiffs have conducted a significant amount of third-party discovery aimed at Georgia's counties and municipalities. Plaintiffs have also asserted a desire to publicly disclose as much information obtained in this litigation as possible. The public disclosure of highly confidential documents and information poses risks to the ongoing security of Georgia's elections, and the protective order should ensure that highly sensitive information remains protected.

As an initial matter, due to how Georgia's elections are conducted and the statutory duties of local elections officials, counties and municipalities are or may be in possession of documents containing sensitive information regarding Georgia's elections. Georgia law contemplates the possession of sensitive information by local officials and limits public access to these documents to ensure election security. *See, e.g.*, O.C.G.A. §§ 21-2-379.24(g); 21-2-500, *see also, e.g.*, *Smith v. Dekalb Cnty.*, 288 Ga. App. 574 (2007) (recognizing the state's security interest in elections information and the Secretary's standing to ensure such security). To avoid claims that State Defendants are attempting to impede third-party discovery by contacting local elections officials about discovery Plaintiffs may seek from them, State Defendants have proposed a protocol that allows parties to appropriately mark sensitive documents "confidential" if third parties produce them without such a designation. Plaintiffs could then challenge any confidential designation by Defendants, similar to the challenge process for other documents Defendants produce with the confidential designation, and the Court could determine whether such documents should be deemed public. *See* [Doc. 429-2 at ¶¶ 2, 7]. This protocol would better ensure that sensitive information in the hands of third parties, namely local elections officials, is protected.

The second issue raised at the June 28, 2019 teleconference involves the scope of the AEO provision to non-attorneys. As the Court recognized at the teleconference, Plaintiffs are committed activists who do not have the same obligations as counsel or an expert. (Trans. at 34:14-23.) Plaintiffs' desire to publicly disclose as much information obtained in this litigation as possible increases the risk that exposing AEO information to the Plaintiffs could result in public disclosure. If sensitive information is subsequently made public, including possibly after the litigation, State Defendants would have no practical way to claw it back. The risk that sensitive information will be released to the public is heightened by allowing Plaintiffs access to that information, and as such, an AEO provision that limits access to sensitive information would be prudent under the circumstances.

Claims that malware *could potentially* get into the voting system should not give anyone an unlimited pass to access the government's critical infrastructure. State Defendants have attempted to balance the need for Plaintiffs' access to sensitive information with State Defendants' important government interest in protecting sensitive, highly confidential information about Georgia's elections infrastructure. State Defendants have offered a prudent, rational approach to discovery by offering to produce information that would allow Plaintiffs' experts

to confirm that no malware exists in Georgia's election system and this Court must not allow unfettered access to this critical infrastructure.

This 1st day of July, 2019.

/s/ Vincent Russo
Vincent R. Russo
GA Bar No. 242628
Josh Belinfante
GA Bar No. 047399
Carey A. Miller
GA Bar No. 976240
Kimberly Anderson
GA Bar No. 602807
Alexander Denton
GA Bar No. 660632
Brian E. Lake
GA Bar No. 575966
ROBBINS ROSS ALLOY
BELINFANTE LITTLEFIELD LLC
500 14th Street NW
Atlanta, GA 30318
Telephone: (678) 701-9381
Facsimile: (404) 856-3250
vrusso@robbinsfirm.com
jbelinfante@robbinsfirm.com
cmiller@robbinsfirm.com
kanderson@robbinsfirm.com
adenton@robbinsfirm.com
blake@robbinsfirm.com

/s/Bryan P. Tyson
Bryan P. Tyson
GA Bar No. 515411
Bryan F. Jacoutot

Georgia Bar No. 668272
TAYLOR ENGLISH DUMA LLP
1600 Parkwood Circle, Suite 200
Atlanta, GA 30339
Telephone: (678)336-7249
btyson@taylorenglish.com
bjacoutot@taylorenglish.com

Counsel for State Defendants

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1(D), the undersigned hereby certifies that the foregoing DEFENDANTS' RESPONSE TO COURT'S REQUEST ON DISCOVERY DISPUTE has been prepared in Times New Roman 14-point, a font and type selection approved by the Court in L.R. 5.1(B).

/s/Bryan P. Tyson
Bryan P. Tyson
GA Bar No. 515411

CERTIFICATE OF SERVICE

I hereby certify that on this day, I electronically filed the foregoing STATE DEFENDANTS' RESPONSE TO COURT'S REQUEST ON DISCOVERY DISPUTE with the Clerk of Court using the CM/ECF system, which will automatically send counsel of record e-mail notification of such filing.

This 1st day of July, 2019.

/s/Bryan P. Tyson
Bryan P. Tyson
GA Bar No. 515411